arXiv:1301.5876v1 [math.NT] 24 Jan 2013

Modular forms, de Rham cohomology and congruences

Matija Kazalicki and Anthony J. Scholl

Abstract

In this paper we show that Atkin and Swinnerton-Dyer type of congruences hold for weakly modular forms (modular forms that are permitted to have poles at cusps). Unlike the case of original congruences for cusp forms, these congruences are nontrivial even for congruence subgroups. As an example, we consider the space of cusp forms of weight 3 on a certain genus zero quotient of Fermat curve $X^N + Y^N = Z^N$. We show that the Galois representation associated to this space is Grossencharacter of a cyclotomic field $\mathbb{Q}(\zeta_N)$. Moreover, for $N = 5$ the space does not admit a "p-adic Hecke eigenbasis" for (non-ordinary) primes $p \equiv 2, 3 \pmod 5$, which provides a counterexample for original Atkin and Swinnerton-Dyer speculaction (see [2], [7], [8]).

1 Introduction

In [2], Atkin and Swinnerton-Dyer described a remarkable family of congruences they had discovered, involving the Fourier coefficients of modular forms on noncongruence subgroups. Their data suggested (see [8] for a precise conjecture) that the spaces of cusp forms of weight k for noncongurence subgroup, for all but finitely many primes p, should posses a p-adic Hecke eigenbasis in the sense that Fourier coefficients $a(n)$ of each basis element satisfy

$$a(pn) - A_p a(n) + \chi(p) p^{k-1} a(n/p) \equiv 0 \pmod{p^{(k-1)(1+\mathrm{ord}_p(n))}},$$

where A_p is an algebraic integer and χ is a Dirichlet character (they depend on basis element, but not on n). This congruence relation is reminiscent of the relation between Fourier coefficients of Hecke eigenforms for congruence subgroups (which is surprising since there is no usefull Hecke theory for modular forms on noncongruence subgroups).

Following work by Cartier [3], Ditters [5] and Katz [6], the second author proved a substantial part of these congruences in [10]. There remain various

questions concerning the optimal shape of these congruences in the case when the dimension of the space of cusp forms is greater than one, see [1, 8, 9].

In this paper we show that similar congruences (also initially discovered experimentally) hold for weakly modular forms (that is, modular forms which are permitted to have poles at cusps). Unlike the case of Atkin–Swinnerton-Dyer's original congruences for cusp forms, these congruences are nontrivial even for congruence subgroups (because the Hecke theory of weakly modular forms is not so good). The simplest case is the weakly modular form of level 1 and weight 12

$$\begin{aligned} E_4(z)^6/\Delta(z) - 1464E_4(z)^3 &= q^{-1} + \sum_{n=1}^{\infty} a(n)q^n \\ &= q^{-1} - 142236q + 51123200q^2 + 39826861650q^3 + \cdots \end{aligned}$$

For every prime $p \geq 11$ and integer n with $p^s|n$, its coefficients satisfy the congruence

$$a(np) - \tau(p)a(n) + p^{11}a(n/p) \equiv 0 \pmod{p^{11s}}.$$

where $\tau(n)$ is Ramanujan's function. (Note that the coefficients $a(n)$ grow too rapidly to satisfy any multiplicative identities.)
More examples may be found in §3 below.

As a further example, for odd integer N, we consider the space of weight 3 cuspforms on a certain genus zero quotient of Fermat curves $X^N + Y^N = Z^N$. These cusp forms are "CM" forms in the sense that the Galois representation associated to them is a Grossencharacter of a cyclotomic field $\mathbb{Q}(\zeta_N)$. We show that for $N = 5$ the space of weight 3 cuspforms does not admit a p-adic Hecke eigenbasis for (non-ordinary) primes $p \equiv 2, 3 \pmod 5$. Moreover, for the better understanding of the congruences arising from the action of Frobenius endomorphism in this situation, we define certain weakly modular forms, and prove some congruences for them. For more details see §11.

In [10] the congruences were obtained by embedding the module of cusp forms of weight k (on a fixed subgroup Γ) into a de Rham cohomology group $DR(X, k)$, where X is the modular curve associated to Γ. This cohomology group is the de Rham realisation of the motive [11] associated to the relevant space of modular forms. At a good prime p, crystalline theory endows $DR(X, k) \otimes \mathbb{Z}_p$ with a Frobenius endomorphism, whose action on q-expansions can be explicitly computed, and this gives rise to the Atkin–Swinnerton-Dyer congruences. (See the introduction of [10] for more explanation.) Here we observe that there is an simple description of $DR(X, k)$ in terms of "forms of the second kind". Curiously, such a description does not appear to be explicitly given anywhere in the literature (although it is implicit in Coleman's work on p-adic modular forms). The period isomorphism is particularly transparent in this interpretation.

2 Summary of results

Let $\Gamma \subset SL_2(\mathbb{Z})$ be a subgroup of finite index. We choose a number field $K = K_\Gamma \subset \mathbb{C}$ and a model X_K over K for the compactified modular curve $\Gamma\backslash\mathfrak{H}^*$ such that:

- the j-function defines a morphism $\pi_K\colon X_K \to \mathbb{P}^1_K$; and
- the cusp $\infty \in \Gamma\backslash\mathfrak{H}^*$ is a rational point of X_K.

Let m be the width of the cusp ∞. Then the completed local ring $\widehat{\mathcal{O}_{X,\infty}}$ equals $K[[t]]$ for some t with $\delta t^m = q$, with $\delta \in K^*$.

Let $X_K^o \subset X_K$ be the complement of the points where the covering $\mathfrak{H} \to X_K(\mathbb{C})$ is ramified. On $X_{\mathbb{C}}^o$ we have the standard line bundle $\underline{\boldsymbol{\omega}}_{\mathbb{C}}$, such that modular forms of weight k are sections of $\underline{\boldsymbol{\omega}}_{\mathbb{C}}^{\otimes k}$, and the canonical isomorphism $\psi_{\mathbb{C}}\colon \underline{\boldsymbol{\omega}}_{\mathbb{C}}^{\otimes 2} \xrightarrow{\sim} \Omega^1_{X_{\mathbb{C}}^o}(\text{log cusps})$, identifying forms of weight 2 with holomorphic 1-forms on $X_{\mathbb{C}}$. The fibre at infinity has a canonical generator $\varepsilon_{\mathbb{C}} \in \underline{\boldsymbol{\omega}}_{\mathbb{C}}(\infty)$. If $-1 \notin \Gamma$ we also assume that this structure comes from a triple $(\underline{\boldsymbol{\omega}}_K, \psi_K, \varepsilon_K \in \underline{\boldsymbol{\omega}}_K(\infty))$ on X_K^o.

We choose a finite set S of primes of K, and write $R = \mathfrak{o}_{K,S}$, satisfying:

- $6m$ and δ are in R^*;
- there exists a smooth projective curve X/R with $X_K = X \otimes_R K$, and π_K extends to a finite morphism $\pi\colon X \to \mathbb{P}^1_R$ which is étale away from $j \in \{\infty, 0, 1728\}$;
- if $-1 \notin \Gamma$, $(\underline{\boldsymbol{\omega}}_K, \psi_K, \varepsilon_K)$ extends to a triple $(\underline{\boldsymbol{\omega}}, \psi, \varepsilon)$ on X^o, with $\underline{\boldsymbol{\omega}}(\infty) = R\varepsilon$.

Any modular or weakly modular form on Γ has a Fourier expansion at ∞ which lies in $\mathbb{C}((q^{1/m})) = \mathbb{C}((t))$. For any subring R' of $\mathbb{C}$ containing R, and any $k \geq 2$, let $S_k(\Gamma, R')$, $M_k(\Gamma, R')$ be the R'-modules of cusp (resp. modular) forms on Γ of weight k whose Fourier expansions at ∞ lie in $R'[[t]]$. Standard theory shows that $S_k(\Gamma, R)$, $M_k(\Gamma, R)$ are locally free R-modules and that, for any R',

$$S_k(\Gamma, R') = S_k(\Gamma, R) \otimes_R R', \quad M_k(\Gamma, R') = M_k(\Gamma, R) \otimes_R R'$$

For any integer s, denote by $M_s^{\mathrm{wk}}(\Gamma, R')$ the R'-module of weakly modular forms (meromorphic at all cusps) of weight s whose Fourier expansions at ∞ lie in $R'((t))$, and let $S_s^{\mathrm{wk}}(\Gamma, R')$ be the submodule consisting of those $f \in M_s^{\mathrm{wk}}(\Gamma, R')$ whose constant term at each cusp vanishes.

It is well known that if $k \geq 2$ there is a linear map

$$\partial^{k-1}\colon M_{2-k}^{\mathrm{wk}}(\Gamma, \mathbb{C}) \to S_k^{\mathrm{wk}}(\Gamma, \mathbb{C})$$

which on Fourier expansions (at any cusp) is given by $(q\, d/dq)^{k-1}$. Consequently ∂^{k-1} maps $M_{2-k}^{\mathrm{wk}}(\Gamma, R')$ into $S_k^{\mathrm{wk}}(\Gamma, R')$.

Definition. Suppose $K \subset K' \subset \mathbb{C}$. Define for $k \geq 2$

$$DR(\Gamma, K', k) = \frac{S_k^{\mathrm{wk}}(\Gamma, K')}{\partial^{k-1}(M_{2-k}^{\mathrm{wk}}(\Gamma, K'))}$$

and

$$DR^*(\Gamma, K', k) = \frac{M_k^{\mathrm{wk}}(\Gamma, K')}{\partial^{k-1}(M_{2-k}^{\mathrm{wk}}(\Gamma, K'))}$$

It is clear that for every K', $DR(\Gamma, K', k) = DR(\Gamma, K, k) \otimes_K K'$, and similarly for DR^*.

If $R \subset R' \subset \mathbb{C}$ and $f \in M_k^{\mathrm{wk}}(\Gamma, R')$, the conditions on S imply that the Fourier coefficients of f at any cusp are integral over R'. Write the Fourier expansion of f at a cusp z of width m as

$$\tilde{f}_z = \sum_{n \in \mathbb{Z}} a_n(f, z) q^{n/m}.$$

Definition. Let $f \in M_k^{\mathrm{wk}}(\Gamma, R')$. We say that f is *weakly exact* if, at each cusp z of Γ, and for each $n < 0$, $n^{-1} a_n(f, z)$ is integral over R'. We write $M_k^{\mathrm{wk-ex}}(\Gamma, R')$ for the R'-module of weakly exact modular forms and $S_k^{\mathrm{wk-ex}}(\Gamma, R')$ for the submodule of weakly exact cusp forms.

It is clear that $\partial^{k-1}(M_{2-k}^{\mathrm{wk}}(\Gamma, R') \subset S_k^{\mathrm{wk-ex}}(\Gamma, R')$.

Definition. Define for $k \geq 2$

$$DR(\Gamma, R', k) = \frac{S_k^{\mathrm{wk-ex}}(\Gamma, R')}{\partial^{k-1}(M_{2-k}^{\mathrm{wk}}(\Gamma, R'))}$$

and

$$DR^*(\Gamma, R', k) = \frac{M_k^{\mathrm{wk-ex}}(\Gamma, R')}{\partial^{k-1}(M_{2-k}^{\mathrm{wk}}(\Gamma, R'))}$$

If $R' \supset \mathbb{Q}$ this obviously agrees with our earlier definition.

In §4, §5, and §6 we will prove that these groups enjoy the following properties.

- The R-modules $DR(\Gamma, R, k)$ and $DR^*(\Gamma, R, k)$ are locally free, and for every $R' \supset R$ we have

  $$DR(\Gamma, R', k) = DR(\Gamma, R, k) \otimes_R R', \quad DR^*(\Gamma, R', k) = DR^*(\Gamma, R, k) \otimes_R R'$$

- There exists for each $k \geq 2$ a commutative diagram with exact rows

  $$\begin{array}{ccccccccc} 0 & \longrightarrow & S_k(\Gamma, R) & \longrightarrow & DR(\Gamma, R, k) & \longrightarrow & S_k(\Gamma, R)^\vee & \longrightarrow & 0 \\ & & \bigcup & & \bigcup & & \| & & \\ 0 & \longrightarrow & M_k(\Gamma, R) & \longrightarrow & DR^*(\Gamma, R, k) & \longrightarrow & S_k(\Gamma, R)^\vee & \longrightarrow & 0 \end{array}$$

  in which all the monomorphisms are the natural ones.

- Suppose that p is prime, and that for some embedding $\mathbb{Z}_p \hookrightarrow \mathbb{C}$, we have $R \subset \mathbb{Z}_p$. Then there are canonical compatible endomorphisms ϕ_p of $DR(\Gamma, \mathbb{Z}_p, k)$, $DR^*(\Gamma, \mathbb{Z}_p, k)$. The characteristic polynomial $H_p(T)$ of ϕ_p on $DR(\Gamma, \mathbb{Z}_p, k)$ has rational integer coefficients, and its roots are p^{k-1}-Weil numbers. Moreover

$$H_p(T) = (\text{constant}) T^{2d_k} H_p(1/p^{k-1}T)$$

where $d_k = \dim S_k(\Gamma)$.

The characteristic polynomial of ϕ_p on $DR^*(\Gamma, \mathbb{Z}_p, k)/DR(\Gamma, \mathbb{Z}_p, k)$ has integer coefficients and its roots are of the form $p^{k-1} \times (\text{root of unity})$.

- Still assume that $R \subset \mathbb{Z}_p$. There is a unique $\gamma_p \in 1 + p\mathbb{Z}_p$ such that $\gamma_p^m = \delta^{p-1}$. Let $\tilde{\phi}_p$ be the endomorphism of $\mathbb{Z}_p((t))$ given by

$$\tilde{\phi}_p \colon \sum a_n t^n \mapsto p^{k-1} \sum a_n \gamma_p^n t^{np}.$$

Then the diagram

$$\begin{array}{ccc} DR^*(\Gamma, \mathbb{Z}_p, k) & \longrightarrow & \dfrac{\mathbb{Z}_p((t))}{\partial^{k-1}\left(\mathbb{Z}_p((t))\right)} \\ {\scriptstyle \phi_p}\big\downarrow & & \big\downarrow{\scriptstyle \tilde{\phi}_p} \\ DR^*(\Gamma, \mathbb{Z}_p, k) & \longrightarrow & \dfrac{\mathbb{Z}_p((t))}{\partial^{k-1}\left(\mathbb{Z}_p((t))\right)} \end{array}$$

commutes.

- Write $\langle k-1 \rangle = \inf\{\operatorname{ord}_p(p^j/j!) \mid j \geq k-1\}$, and let

$$\begin{aligned} DR^*(\Gamma, \mathbb{Z}_p, k)^{(p)} &= M_k(\Gamma, \mathbb{Z}_p) + p^{\langle k-1 \rangle} DR^*(\Gamma, \mathbb{Z}_p, k) \\ &\subset \frac{M_k^{\text{wk-ex}}(\Gamma, R')}{p^{\langle k-1 \rangle} \partial^{k-1}(M_{2-k}^{\text{wk}}(\Gamma, R'))} \end{aligned}$$

Then ϕ_p preserves $DR^*(\Gamma, \mathbb{Z}_p, k)^{(p)}$ and the diagram

$$\begin{array}{ccc} DR^*(\Gamma, \mathbb{Z}_p, k)^{(p)} & \longrightarrow & \dfrac{\mathbb{Z}_p((t))}{p^{\langle k-1 \rangle}\partial^{k-1}\left(\mathbb{Z}_p((t))\right)} \\ {\scriptstyle \phi_p}\big\downarrow & & \big\downarrow{\scriptstyle \tilde{\phi}_p} \\ DR^*(\Gamma, \mathbb{Z}_p, k)^{(p)} & \longrightarrow & \dfrac{\mathbb{Z}_p((t))}{p^{\langle k-1 \rangle}\partial^{k-1}\left(\mathbb{Z}_p((t))\right)} \end{array}$$

commutes.

Congruences

We continue to assume that $R \subset \mathbb{Z}_p$. Let $\mathfrak{o} = \mathfrak{o}_F$ for a finite extension $F/\mathbb{Q}_p$. Extend ϕ_p to a $\mathfrak{o}$-linear endomorphism of $DR^*(\Gamma, \mathfrak{o}, k)$. Let $f \in M_k^{\mathrm{wk-ex}}(\Gamma, \mathfrak{o})$, with Fourier expansion at infinity

$$\tilde{f} = \sum_{n \in Z} a(n) q^{n/m} = \sum_{n \in \mathbb{Z}} b(n) t^n, \quad b(n) \in \mathfrak{o}.$$

Let $H = \sum_{j=0}^{r} A_j T^j \in \mathfrak{o}[T]$ such that the image of f in $DR^*(\Gamma, \mathfrak{o}, k)$ is annihilated by $H(\phi_p)$.

Theorem 2.1. *(i) The coefficients $a(n)$ satisfy the congruences: if $n \in \mathbb{Z}$ and $p^s | n$ then*

$$\sum_{j=0}^{r} p^{(k-1)j} A_j a(n/p^j) \equiv 0 \pmod{p^{(k-1)s}}.$$

(ii) If moreover $f \in M_k(\Gamma, \mathfrak{o})$ then these congruences hold mod $p^{(k-1)s + \langle k-1 \rangle}$.

Here the left hand side is interpreted as

$$\delta^{-n/m} \sum_{j=0}^{r} p^{(k-1)j} A_j \gamma_p^{n(p^j-1)/(p-1)} b(n/p^j) \in \delta^{-n/m}$$

which is the product of a unit an an element of $\mathfrak{o}$, and we adopt the usual convention that $a(n) = b(n) = 0$ is $n \notin \mathbb{Z}$ (cf. [10, Thm. 5.4]).

Proof. The properties above show that

$$\sum c_n t^n := H(\tilde{\phi})(\tilde{f}) \in \partial^{k-1} \left(\mathfrak{o}((t)) \right)$$

or equivalently that for every $n \in \mathbb{Z}$, $c_n \in n^{k-1}\mathfrak{o}$. Applying $H(\tilde{\phi})$ to $\tilde{f}$ term-by-term, one obtains the congruences (i). If $f \in M_k(\Gamma, \mathfrak{o})$ then $H(\tilde{\phi})(\tilde{f}) \in p^{\langle k-1 \rangle} \operatorname{Im}(\partial^{k-1})$, giving the stronger congruences (ii). $\square$

3 Examples

Under the hypotheses of Theorem 6.4, suppose that $\dim S_k(X \otimes \mathbb{Q}) = 1$ and that $f \in S_k^{\mathrm{wk-ex}}(X)$. Then the characteristic polynomial of ϕ_p on $DR(X \otimes \mathbb{Z}_p, k)$ is of the form

$$H_p(T) = T^2 - A_p T + p^{k-1}, \quad A_p \in \mathbb{Z}$$

The congruences (6.3) then take the form

$$a(np) \equiv A_p a(n) - p^{k-1} a(n/p) \mod p^{(k-1)s} \quad \text{if } p^s | n \tag{3.1}$$

Consider the weak cusp form of level one and weight 12

$$f = E_4(z)^6/\Delta(z) - 1464E_4(z)^3.$$

We cannot directly apply the theorem to f, since the modular curve of level 1 does belong to the class of X considered in §4. We can get round this in the usual way (cf. part (b) proof of [10, 5.2]): take $X = X' = X(3)$ for some auxiliary integer $N \geq 3$, and define $DR(X(1) \otimes \mathbb{Z}[1/6], k) = DR(X(3), k)^{GL(2,\mathbb{Z}/3\mathbb{Z})}$, which is then a free $Z[1/6]$-module of rank 2. For each $p > 3$, $DR(X(1) \otimes \mathbb{Z}_p, 12)$ is annihilated by $H_p(\phi) = \phi^2 - \tau(p)\phi + p^{11}$, and one recovers, for $p \geq 11$, the congruences of the introduction. (With more care we could get congruences for small primes as wll.)

As a further example, consider the following (weakly) modular forms of weight 3 for noncongurence subgroup $\Phi_0(3)$ (see §7 for definition and basic properties).

$$\begin{aligned} f_1(\tau) &= \eta(\tau/2)^{\frac{4}{3}}\eta(\tau)^{-2}\eta(2\tau)^{\frac{20}{3}} \\ &= \sum c_1(n)q^{\frac{n}{2}} = q^{\frac{1}{2}} - \frac{4}{3}q^{\frac{2}{2}} + \frac{8}{9}q^{\frac{3}{2}} - \frac{176}{81}q^{\frac{4}{2}} + \cdots \in S_3(\Phi_0(3)), \end{aligned}$$

$$\begin{aligned} f_2(\tau) &= \eta(\tau/2)^{\frac{20}{3}}\eta(\tau)^{-10}\eta(2\tau)^{\frac{28}{3}} \\ &= \sum c_2(n)q^{\frac{n}{2}} = q^{\frac{1}{2}} - \frac{20}{3}q^{\frac{2}{2}} + \frac{200}{9}q^{\frac{3}{2}} - \frac{4720}{81}q^{\frac{4}{2}} + \cdots \in S_3^{\mathrm{wk}}(\Phi_0(3)). \end{aligned}$$

From Corollary 11.3 it follows that for a prime $p \equiv 2 \bmod 3$, there exist $\alpha_p, \beta_p \in \mathbb{Z}_p$ such that if $p^s|n$ then

$$c_1(pn) \equiv \alpha_p c_2(n) \bmod p^{2(s+1)},$$

$$c_2(pn) \equiv \beta_p c_1(n) \bmod p^{2(s+1)}.$$

Moreover $\alpha_p\beta_p = p^2$, and $\mathrm{ord}_p(\alpha_p) = 2$.

If $p \equiv 1 \bmod 3$, then for some $\alpha_p \in \mathbb{Z}_p$ ($\mathrm{ord}_p(\alpha_p) = 2$), then

$$\begin{aligned} c_1(pn) &\equiv \frac{p^2}{\alpha_p}c_1(n) \bmod p^{2(s+1)}, \\ c_2(pn) &\equiv \alpha_p c_2(n) \bmod p^{2(s+1)}. \end{aligned}$$

For any $p > 3$ we have

$$c_2(pn) - A_p c_2(n) + \chi_3(p)p^2 c_2(n/p) \equiv 0 \bmod p^{2s} \quad \text{if } p^s|n,$$

where A_p is p-th Fourier coefficients of the CM newform on $S_3(\Gamma_1(12))$, and χ_3 is Dirichlet character of conductor 3 (also $H_p(T) = T^2 - A_pT + \chi_3(p)p^2$).

4 Review of [10]

Let R be a field or Dedekind domain of characteristic zero. In this section we will work with modular curves over R. Let X be a smooth projective curve over R, whose fibres need not be geometrically connected, equipped with a finite morphism $g\colon X \to X'$, whose target X' is a modular curve for a representatable moduli problem. In practice we have in mind for X' the basechange from $\mathbb{Z}[1/N]$ to R of one of the following curves:

(i) $X_1(N)$ (for some $N \geq 5$), the modular curve over $\mathbb{Z}[1/N]$ parameterising (generalised) elliptic curves with a section of order N;

(ii) $X(N)$ (for some $N \geq 3$), parameterising elliptic curves with a full level N structure $\alpha\colon (\mathbb{Z}/N)^2 \to E$,

(iii) $X(N)^{\mathrm{arith}}$ (for some $N \geq 3$), parameterising elliptic curves with "arithmetic level N structure of determinant one" $\alpha\colon \mathbb{Z}/N \times \boldsymbol{\mu}_N \to E$

and we will limit ourselves to these cases, although most things should work if X' is replaced by some other modular curve (perhaps for an "exotic" moduli problem).

We let $Y' \subset X'$ be the open subset parameterising true elliptic curves, and $Z' \subset X'$ the complementary reduced closed subscheme (the cuspidal subscheme). We make the following hypotheses on the morphism g:

(A) $g\colon X \to X'$ is étale over Y'
(B) $\Gamma(X, \mathcal{O}_X) = K$ is a field.

We write Y, Z for the (reduced) inverse images of Y', Z' in X, and $j\colon Y \hookrightarrow X$ for the inclusion.

A *cusp* is a connected component $z \subset Z$. The hypotheses imply (by Abhyankar's lemma) that $z = \operatorname{Spec} R_z$, where R_z/R is finite and étale. One knows that a formal uniformising parameter along a cusp of X' may be taken to be $q^{1/m}$ for some $m|N$, and we may choose therefore a parameter $t_z \in \widehat{\mathcal{O}_{X,z}}$ such that $\delta_z t_z^{m_z} = q$ for some $m_z \geq 1$, $\delta_z \in R_z^*$. Moreover m_z (the *width* of the cusp z) is invertible in R.

Because Y' represents a moduli problem, there is a universal elliptic curve $\pi\colon E' \to Y'$, which in each of the cases (i–iii) extends to a stable curve of genus one $\bar{\pi}\colon \bar{E}' \to X'$, with a section $e\colon X' \to \bar{E}'$ extending the zero section of E'. We let $\underline{\boldsymbol{\omega}}_{X'} = e^*\Omega^2_{\bar{E}'/X'}$ be the cotangent bundle along e, and $\underline{\boldsymbol{\omega}}_X$ its pullback to X.

If U is any R-scheme we shall simply write Ω^1_U for the module of relative differentials $\Omega^!_{U/R}$.

The module of (R-valued) modular forms of weight $k \geq 0$ on X is by definition

$$M_k(X) = H^0(X, \underline{\boldsymbol{\omega}}_X^{\otimes k}).$$

There is a well-known canonical "Kodaira–Spencer" isomorphism

$$KS(X')\colon \underline{\boldsymbol{\omega}}_{X'}^{\otimes 2} \xrightarrow{\sim} \Omega^1_{X'}(\log Z').$$

Hypothesis (A) implies that $g^*\Omega^1_{X'}(\log Z') = \Omega^1_X(\log Y)$, and therefore $KS(X')$ pulls back to give an isomorphism

$$KS(X)\colon \underline{\boldsymbol{\omega}}_{X}^{\otimes 2} \xrightarrow{\sim} \Omega^1_{X}(\log Z).$$

One therefore has

$$M_k(X) = H^0(X, \underline{\boldsymbol{\omega}}_X^{\otimes k-2} \otimes \Omega^1_X(\log Z))$$

and the submodule of cusp forms is

$$S_k(X) = H^0(X, \underline{\boldsymbol{\omega}}_X^{\otimes k-2} \otimes \Omega^1_X).$$

Serre duality then gives a canonical isomorphism of free R-modules

$$S_k(X)^\vee \xrightarrow{\sim} H^1(X, \underline{\boldsymbol{\omega}}_X^{\otimes 2-k}).$$

The relative de Rham cohomology of the family $E' \to Y'$ is a rank 2 locally free sheaf $\mathcal{E}_{Y'} = R^1\pi_*\Omega^*_{E'/Y'}$, which carries an integrable connection ∇. Denote by $\underline{\boldsymbol{\omega}}_Y$, $\mathcal{E}_Y$ the pullbacks of $\underline{\boldsymbol{\omega}}_{Y'}$, $\mathcal{E}_{Y'}$ to Y.

There is a canonical extension (in the sense of [4]) of $(\mathcal{E}_{Y'}, \nabla)$ to a locally free sheaf $\mathcal{E}_{X'}$ with logarithmic connection

$$\nabla\colon \mathcal{E}_{X'} \to \mathcal{E}_{X'} \otimes \Omega^1_{X'}(\log Z')$$

whose residue map Res_∇ — defined by the commutativity of the square

$$\begin{tikzcd}
\mathcal{E}_{X'} \arrow[r, "\nabla"] \arrow[d, "(-)\otimes 1"'] & \mathcal{E}_{X'} \otimes \Omega^1_{X'}(\log Z') \arrow[d, "id\otimes \mathrm{Res}_{Z'}"] \\
\mathcal{E}_{X'} \otimes \mathcal{O}_{Z'} \arrow[r, "\mathrm{Res}_\nabla"] & \mathcal{E}_{X'} \otimes \mathcal{O}_{Z'}
\end{tikzcd}$$

— is nilpotent. The canonical extension may be described explicitly using the Tate curve: in the cases (i–iii), each cusp $z \subset Z'$ is the spectrum of a cyclotomic extension $R' = R[\zeta_M]$ (for some $M|N$ depending on z). The basechange of E' to $R'((q^{1/m}))$ via the q-expansion map is canonically isomorphic to the pullback of the Tate curve $\mathrm{Tate}(q)/\mathbb{Z}[1/N]((q^{1/m}))$, and there is a canonical basis

$$H^1_{\mathrm{dR}}(\mathrm{Tate}(q)/\mathbb{Z}[1/N]((q^{1/m}))) = \mathbb{Z}[1/N]((q^{1/m}))\cdot\omega_{\mathrm{can}} \oplus \mathbb{Z}[1/N]((q^{1/m}))\cdot\xi_{\mathrm{can}}$$
$$\nabla(\omega_{\mathrm{can}}) = \xi_{\mathrm{can}} \otimes dq/q, \quad \nabla(\xi_{\mathrm{can}}) = 0$$

for the de Rham cohomology of the Tate curve. The canonical extension of $\mathcal{E}_{Y'}$ to X' is then the unique extension for which, at each cusp z as above,

$\widehat{\mathcal{E}}_{X',x}$ is generated by ω_{can} and ξ_{can}. In particular, in the basis $(\omega_{\mathrm{can}}, \xi_{\mathrm{can}})$ the residue map at a cusp z of width m has matrix

$$\mathrm{Res}_{\nabla,z} = \begin{pmatrix} 0 & 0 \\ m & 0 \end{pmatrix}.$$

We write $\underline{\boldsymbol{\omega}}_X$, $\mathcal{E}_X$ for the pullbacks of $\underline{\boldsymbol{\omega}}_{X'}$, $\mathcal{E}_{X'}$ to X. Since the residues are nilpotent, $\mathcal{E}_X$ is equal to the canonical extension of $\mathcal{E}_Y$.

The Hodge filtration of $\mathcal{E}_{Y'}$ extends to give a short exact sequence

$$0 \longrightarrow F^1\mathcal{E}_X = gr^1_F\mathcal{E}_X = \underline{\boldsymbol{\omega}} \longrightarrow F^0 = \mathcal{E}_X \longrightarrow \underline{\boldsymbol{\omega}}^\vee \longrightarrow 0$$

and the Kodaira-Spencer map is obtained (by tensoring with $\underline{\boldsymbol{\omega}}$) from the composite

$$\underline{\boldsymbol{\omega}}_X \hookrightarrow \mathcal{E}_X \xrightarrow{\nabla} \mathcal{E}_X \otimes \Omega^1_X(\log Z) \to \underline{\boldsymbol{\omega}}_X^\vee \otimes \Omega^1_X(\log Z)$$

In [10], some de Rham cohomology groups associated to modular forms were defined. Define, for an integer $k \geq 2$,

$$\Omega^0(\mathcal{E}_X^{(k-2)}) = \mathcal{E}_X^{(k-2)} := \mathrm{Sym}^{k-2}\,\mathcal{E}_X,$$
$$\Omega^1(\mathcal{E}_X^{(k-2)}) := \nabla(\mathcal{E}_X^{(k-2)}) + \mathcal{E}_X^{(k-2)} \otimes \Omega^1_X \subset \mathcal{E}_X^{(k-2)} \otimes \Omega^1_X(\log Z)$$

and let

$$\nabla^{(k-2)} \colon \Omega^0(\mathcal{E}_X^{(k-2)}) \to \Omega^1(\mathcal{E}_X^{(k-2)})$$

be the $(k-2)$-th symmetric power of the connection ∇. This makes $\Omega^\bullet(\mathcal{E}_X^{(k-2)})$ into a complex of locally free $\mathcal{O}_X$-modules with R-linear maps. Define

$$DR(Y,k) := H^1(X, \mathcal{E}_X^{(k-2)} \otimes \Omega^*_X(\log Z)),$$
$$DR(X,k) := H^1(X, \Omega^\bullet(\mathcal{E}_X^{(k-2)})) \tag{4.1}$$

In the notation of §2 of [10], $DR(X,k) = L_{k-2}(X,R)$ and $DR(Y,k) = T_{k-2}(X,R)$.

The Hodge filtration on $\mathcal{E}_X^{(k-2)}$ is the symmetric power of the Hodge filtration $F^\bullet$ on $\mathcal{E}_X$: its associated graded is

$$\mathrm{gr}^j_F\,\mathcal{E}_X^{(k-2)} = \begin{cases} \underline{\boldsymbol{\omega}}_X^{\otimes(k-2-2j)} & \text{if } 0 \leq j \leq k-2 \\ 0 & \text{otherwise} \end{cases}.$$

Define the filtration $F^\bullet$ on the complex $\mathcal{E}_X^{(k-2)} \otimes \Omega^\bullet_X(\log Z)$ by

$$F^j(\mathcal{E}_X^{(k-2)} \otimes \Omega^i_X(\log Z)) = F^{j-i}(\mathcal{E}_X^{(k-2)}) \otimes \Omega^i_X(\log Z).$$

Then the connection $\nabla^{(k-2)}$ respects $F^\bullet$. On the associated graded, $\nabla^{(k-2)}$ is $\mathcal{O}_X$-linear, and if $(k-2)!$ is invertible in R, away from the extreme degrees it is an isomorphism:

$$\begin{gathered}
\mathrm{gr}^0_F(\mathcal{E}_Y^{(k-2)} \otimes \Omega^\bullet_X(\log Z)) = \underline{\boldsymbol{\omega}}_X^{\otimes 2-k} \\
\mathrm{gr}^{k-1}_F(\mathcal{E}_Y^{(k-2)} \otimes \Omega^\bullet_X(\log Z)) = \underline{\boldsymbol{\omega}}_X^{\otimes k-2} \otimes \Omega^1_X(\log Z)[-1] \\
\mathrm{gr}^j_F \nabla^{(k-2)} \colon \mathrm{gr}^j_F \mathcal{E}_X^{(k-2)} \xrightarrow{\sim} \mathrm{gr}^{j-1}_F \mathcal{E}_X^{(k-2)} \otimes \Omega^1_X(\log Z) \qquad \text{if } 0 < j < k-1
\end{gathered}$$

In fact, $\mathrm{gr}^j_F \nabla^{(k-2)} = j(KS \otimes id_{\underline{\boldsymbol{\omega}}^{\otimes k-2j}})$ if $0 < j < k-1$. Therefore from the spectral sequences for the cohomology of the filtered complexes

$$(\mathcal{E}_Y^{(k-2)} \otimes \Omega^\bullet_X(\log Z), F^\bullet) \quad \text{and} \quad (\Omega^\bullet(\mathcal{E}_X^{(k-2)}), F^\bullet)$$

we obtain a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & S_k(X) & \longrightarrow & DR(X,k) & \longrightarrow & S_k(X)^\vee & \longrightarrow & 0 \\
 & & {\scriptstyle\subset}\big\downarrow & & \big\downarrow & & \big\| & & \\
0 & \longrightarrow & M_k(X) & \longrightarrow & DR(Y,k) & \longrightarrow & S_k(X)^\vee & \longrightarrow & 0
\end{array}$$

and

$$H^j(X, \Omega^\bullet(\mathcal{E}_X^{(k-2)})) = H^j(X, \mathcal{E}_X^{(k-2)} \otimes \Omega^\bullet_X(\log Z)) = 0 \quad \text{if } j \neq 1,\ k > 0.$$

More precisely, there are isomorphisms in the derived category

$$\mathcal{E}_Y^{(k-2)} \otimes \Omega^\bullet_X(\log Z) = \left[\ \underline{\boldsymbol{\omega}}_X^{\otimes 2-k} \xrightarrow{\mathcal{D}^{k-1}} \underline{\boldsymbol{\omega}}_X^{\otimes k-2} \otimes \Omega^1_X(\log Z)\ \right] \tag{4.2}$$

$$\Omega^\bullet(\mathcal{E}_X^{(k-2)}) = \left[\ \underline{\boldsymbol{\omega}}_X^{\otimes 2-k} \xrightarrow{\mathcal{D}^{k-1}} \underline{\boldsymbol{\omega}}_X^{\otimes k-2} \otimes \Omega^1_X\ \right] \tag{4.3}$$

where $\mathcal{D}^{k-1}$ is a differential operator which is characterised by its effect on q-expansion:

$$\mathcal{D}^{k-1}(f\,\omega_{\mathrm{can}}^{2-k}) = \frac{(-1)^k}{(k-2)!}\Big(d\frac{d}{dq}\Big)^{k-1}(f)\,\omega_{\mathrm{can}}^{k-2} \otimes \frac{dq}{q}$$

(see [10, proof of 2.7(ii)]).

Finally note that from the exact sequence of complexes

$$0 \longrightarrow \Omega^\bullet(\mathcal{E}_X^{(k-2)}) \longrightarrow \mathcal{E}_X^{(k-2)} \otimes \Omega^\bullet_X(\log Z) \xrightarrow{\mathrm{Res}_Z} \underline{\boldsymbol{\omega}}_X^{\otimes k-2} \otimes \mathcal{O}_Z \longrightarrow 0$$

we obtain an exact sequence

$$0 \longrightarrow DR(X,k) \longrightarrow DR(Y,k) \xrightarrow{\mathrm{Res}} \Gamma(Z, \underline{\boldsymbol{\omega}}_X^{\otimes k-2} \otimes \mathcal{O}_Z) \longrightarrow 0$$

5 Modular forms of the second and third kind

For any $k \in \mathbb{Z}$, and any R, define

$$M_k^{\mathrm{wk}}(X) := \Gamma(Y, \underline{\boldsymbol{\omega}}_Y^k),$$

the R-module of meromorphic modular forms[1] of weight k on X. We say that an element of $M_k^{\mathrm{wk}}(X)$ is a meromorphic cusp form if, at each cusp, its q-expansion has vanishing constant term. Let $S_k^{\mathrm{wk}}(X) \subset M_k^{\mathrm{wk}}(X)$ denote the submodule of meromorphic cusp forms.

Composing $\mathcal{D}^{k-1}$ with the Kodaira-Spencer isomorphism we obtain a R-linear map

$$\theta^{k-1} \colon M_{2-k}^{\mathrm{wk}}(X) \to M_k^{\mathrm{wk}}(X)$$

which on q-expansions is given by $(q\,d/dq)^{k-1}$, and whose image is contained in $S_k^{\mathrm{wk}}(X)$.

Suppose $R = K$ is a field. Then one knows (cf. [4]) that the restriction map

$$H^*(X, \mathcal{E}_X^{(k-2)} \otimes \Omega_X^\bullet(\log Z)) \to H^*(Y, \mathcal{E}_Y^{(k-2)} \otimes \Omega_Y^\bullet)$$

is an isomorphism, and since Y is affine, the cohomology group on the right can be computed as the cohomology of the complex of groups of global sections.

We therefore have the following description of the de Rham cohomology groups as "forms of the second and third kind":

Theorem 5.1. *If R is a field, there exist canonical isomorphisms*

$$DR(Y,k) = \frac{M_k^{\mathrm{wk}}(X)}{\theta^{k-1}(M_{2-k}^{\mathrm{wk}}(X))}, \qquad DR(X,k) = \frac{S_k^{\mathrm{wk}}(X)}{\theta^{k-1}(M_{2-k}^{\mathrm{wk}}(X))}$$

compatible with the inclusions on both sides. The Hodge filtrations on $DR(Y,k)$ and $DR(X,k)$ are induced by the inclusion $M_k(X) \subset M_k^{\mathrm{wk}}(X)$.

Remarks. (i) When $k = 2$ we simply recover the classical formulae for the first de Rham cohomology of a smooth affine curve $Y = X \setminus Z$ over a field of characteristic zero:

$$H^1_{\mathrm{dR}}(Y/K) = \frac{\Gamma(Y, \Omega_Y^1)}{d\,(\Gamma(Y, \mathcal{O}_Y))}$$

and for the complete curve X

$$H^1_{\mathrm{dR}}(X/K) = \frac{\{\text{forms of the 2nd kind on } X, \text{ regular on } Y\}}{d\,(\Gamma(Y, \mathcal{O}_Y))}$$

[1] Often called "weakly modular forms"

(ii) Suppose $K = \mathbb{C}$ and $Y(\mathbb{C}) = \Gamma\backslash\mathfrak{H}$ is a classical modular curve. Then one has a natural isomorphism from $DR(X, K)$ to Eichler–Shimura parabolic cohomology [13] given by periods:

$$f(z) \mapsto \left(\int_{z_0}^{\gamma(z_0)} P(z,1) f(z)\, dz \right)_{\gamma}$$

for homogeneous $P \in \mathbb{C}[T_0, T_1]$ of degree $(k-2)$.

For general R, the description given in the theorem needs to be modified. Since the R-modules $DR(Y, k)$ and $DR(X, k)$ are locally free, and their formation commutes with basechange, restriction to Y induces an injective map

$$DR(Y, k) \to \frac{M_k^{\mathrm{wk}}(X)}{\theta^{k-1}(M_{2-k}^{\mathrm{wk}}(X))}. \tag{5.2}$$

For each cusp $z \subset Z$, let $R_z = \Gamma(z, \mathcal{O}_z)$ and let $t_z \in \widehat{\mathcal{O}_{X,z}}$ be a uniformising parameter on X along z. Say that $f \in M_k^{\mathrm{wk}}(X)$ is *weakly exact* if for every cusp z, the principal part of f at z is in the image of θ^{k-1}. Explicitly, if the expansion of f at z is $\sum a_n t_z^n \otimes \omega_{\mathrm{can}}^{\otimes k}$, the condition is that $a_n \in n^{k-1} R_z$ for every $n < 0$. Let

$$S^{\mathrm{wk-ex}}(X) \subset M_k^{\mathrm{wk-ex}}(X) \subset M_k^{\mathrm{wk}}(X)$$

denote the submodules of weakly exact cusp and modular forms, respectively.

If $g \in M_{2-k}^{\mathrm{wk}}(X)$ then evidently $\theta^{k-1}(g)$ is weakly exact.

Theorem 5.3. *For any R the maps* (5.2) *induce isomorphisms*

$$DR(X, k) = \frac{S_k^{\mathrm{wk-ex}}(X)}{\theta^{k-1}(M_{2-k}^{\mathrm{wk}}(X))}, \qquad DR(X, k) = \frac{S_k^{\mathrm{wk-ex}}(X)}{\theta^{k-1}(M_{2-k}^{\mathrm{wk}}(X))}.$$

Proof. Let $X_{/Z} = \operatorname{Spec} \widehat{\mathcal{O}_{X,Z}}$ denote the formal completion of X along Z, and $Y_{/Z} = X_{/Z} - Z$ the complement; thus

$$X_{/Z} = \coprod_z \operatorname{Spec} R_z[[t_z]] \supset Y_{/Z} = \coprod_z \operatorname{Spec} R_z((t_z)).$$

Then $Y \coprod X_{/Z}$ is a faithfully flat affine covering of X, and so its Cech complex computes the cohomology of any complex of coherent $\mathcal{O}_X$-modules with R-linear maps. Applying this to the complex (4.2), we see that $DR(X, k)$ is the H^1 of the double complex of R-modules:

$$\begin{array}{ccc}
\Gamma(Y_{/Z}, \underline{\boldsymbol{\omega}}^{2-k}) & \xrightarrow{\theta^{k-1}} & \Gamma(Y_{/Z}, \underline{\boldsymbol{\omega}}^{k}) \\
\uparrow & & \uparrow \\
M_{2-k}^{\mathrm{wk}}(X) \oplus \Gamma(X_{/Z}, \underline{\boldsymbol{\omega}}^{2-k}) & \xrightarrow{\theta^{k-1}} & S_k^{\mathrm{wk}}(X) \oplus \Gamma(X_{/Z}, \underline{\boldsymbol{\omega}}^{k})
\end{array}$$

or equivalently as the H^1 of the complex

$$M_k^{\rm wk}(X) \xrightarrow{\theta^{k-1}} S_k^{\rm wk}(X) \xrightarrow{\beta} \frac{\Gamma(Y_{/Z}, \underline{\boldsymbol{\omega}}^k)}{\Gamma(X_{/Z}, \underline{\boldsymbol{\omega}}^k) + \theta^{k-1}\Gamma(Y_{/Z}, \underline{\boldsymbol{\omega}}^{2-k})}$$

and $S_k^{\rm wk-ex}(X)$ is precisely $\ker(\beta)$. Likewise for $DR(Y,k)$. □

6 q-expansions and crystalline structure

Let $z \subset Z$ be a cusp, and write

$$\partial = q\frac{d}{dq} = m_z t_z \frac{d}{dt_z},$$

a derivation of $R_z((t_z))$. We have the local expansion maps

$$\mathrm{loc}_z\colon DR(X,k) \to \frac{R_z[[t_z]]}{\partial^{k-1}(R_z[[t_z]])}, \quad DR(Y,k) \to \frac{R_z((t_z))}{\partial^{k-1}(R_z((t_z))}$$

such that the restriction of $f \in DR(X,k)$ to the formal neighbourhood of z is $\mathrm{loc}_z(f) \otimes \omega_{\rm can}^{\otimes k}$.

Suppose now that $R = \mathfrak{o}_K$ for a finite unramified extension $K/\mathbb{Q}_p$, and let σ be the arithmetic Frobenius automorphism of K. For each z, denote also by σ the Frobenius automorphism of R_z (which is also an unramified extension of $\mathbb{Z}_p$). By Hensel's lemma there is a unique γ_z with

$$\gamma_z \in 1 + pR_z \quad \text{and} \quad \gamma_z^{m_z} = \delta_z^p/\sigma(\delta_z).$$

The σ-linear endomorphism $q \mapsto q^p$ of $R((q))$ then extends to a unique σ-linear endomorphism of $R_z((t_z))$ whose reduction is Frobenius, given by

$$t_z \mapsto \gamma_z t_z^p$$

Then, as explained in §3 of [10], there are compatible σ-linear endomorphisms ϕ of $DR(X,k)$ and $DR(Y,k)$, with the property that

$$\mathrm{loc}_z(f) = \sum a_n t_z^n \quad \Longrightarrow \quad \mathrm{loc}_z(\phi(f)) = p^{k-1}\sum \sigma(a_n)\gamma_z^n t_z^{np} \tag{6.1}$$

Let us assume that $R = \mathbb{Z}_p$, so that ϕ is now linear. Let $z \subset Z$ be a cusp with $R_z = \mathbb{Z}_p$. If $f \in M_k^{\rm wk-ex}(X)$, write the local expansion of f at z as

$$f = \tilde{f} \otimes \omega_{\rm can}^{\otimes k}, \quad \tilde{f} = \sum b(n) t_z^n = \sum a(n) q^{n/m_z}, \quad b(n) = \delta_z^{n/m_z} a(n) \in \mathbb{Z}_p. \tag{6.2}$$

Suppose that $H(T) = \sum_{j=0}^r T^j \in \mathbb{Z}_p[T]$ satisfies $H(\phi)(f) = 0$ in $DR(Y,k)$. Then $\mathrm{loc}_z(H(\phi)f) = 0$, which is equivalent to the following congruences: if $p^s | n$ then

$$\sum_{j=0}^r p^{(k-1)j} A_j a(n/p^j) \equiv 0 \mod p^{(k-1)s}. \tag{6.3}$$

Here we follow the usual convention that $a(n) = b(n) = 0$ for n not an integer, and the left hand side is interpreted as

$$\delta_z^{-n/m_z} \sum_{j=0}^{r} p^{(k-1)j} A_j \gamma_p^{n(p^j-1)/(p-1)} b(n/p^j) \in \delta_z^{-n/m_z} \mathbb{Z}_p$$

cf. [10, Thm, 5.4]. Putting this together we obtain the following extension of the ASD congruences to weakly modular forms:

Theorem 6.4. *Suppose that $R = \mathbb{Z}[1/M]$ and that z is a cusp with $R_z = R$. Let $f \in M_k^{\mathrm{wk-ex}}(X)$, with local expansion at z (6.2). Let p be a prime not dividing M with $p > k-2$, and suppose that the image of f in $DR(Y \otimes \mathbb{Z}_p, k)$ is annihilated by $H(\phi)$ for some polynomial $H(T) = \sum_{j=0}^{r} A_j T^j \in \mathbb{Z}_p[T]$. then for every integer n the congruences (6.3) hold.*

7 Fermat group and modular forms

Modular function and modular forms on Fermat curves have been studied by D.Rohrlich [12] and T. Yang [14]. We follow notation of [14].

Let Δ be the free subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by the matrices $A := \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ and $B := \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)$. One has that $\Gamma(2) = \{\pm I\}\Delta$. Given a positive integer N, the Fermat group $\Phi(N)$ is defined to be the subgroup of Δ generated by A^N, B^N, and the commutator $[\Delta, \Delta]$. It is known that the modular curve $X(\Phi(N))$ is isomorphic to the Fermat curve $X^N + Y^N = 1$. The group $\Phi(N)$ is a congruence group only if $N = 1, 2, 4$ and 8.

Let $N > 1$ be an odd integer. Denote by $\Phi_0(N)$ a group generated by $\Phi(N)$ and A. It is a genus zero index N subgroup of Δ. (The other two genus zero index N subgroups of Δ that contain $\Phi(N)$ are generated by $\Phi(N)$ and AB^{-1} and B respectively.) Associated $X(\Phi_0(N)$ is a quotient of Fermat curve isomorphic to

$$v^N = \frac{u}{1-u},$$

where $u = X^N$ and $v = \frac{X}{Y}$. Denote by $\mathbb{H}$ the complex upper half-plane. If $\tau \in \mathbb{H}$ and $q = e^{2\pi i \tau}$, then

$$\tilde{\lambda}(\tau) = -\frac{1}{16} q^{-1/2} \prod_{n=1}^{\infty} \left(\frac{1 - q^{n-1/2}}{1 + q^n} \right)^8, \tag{7.1}$$

$$1 - \tilde{\lambda}(\tau) = \frac{1}{16} q^{-1/2} \prod_{n=1}^{\infty} \left(\frac{1 + q^{n-1/2}}{1 + q^n} \right)^8 \tag{7.2}$$

are modular functions for $\Gamma(2)$. Moreover, they are holomorphic on $\mathbb{H}$, and $\tilde{\lambda}(\tau) \neq 0, 1$ for all $\tau \in \mathbb{H}$. It follows that there exist holomorphic functions

$\tilde{x}(\tau)$ and $\tilde{y}(\tau)$ on $\mathbb{H}$, such that $\tilde{x}(\tau)^N = \tilde{\lambda}(\tau)$ and $\tilde{y}(\tau)^N = 1 - \tilde{\lambda}(\tau)$, so we have that

$$\tilde{x}(\tau)^N + \tilde{y}(\tau)^N = 1.$$

It turns out that both $\tilde{x}(\tau)$ and $\tilde{y}(\tau)$ are modular functions for $\Phi(N)$. We normalize $\tilde{x}(\tau)$ and $\tilde{y}(\tau)$ by setting

$$x(\tau) := (-1)^{\frac{1}{N}} 16^{\frac{1}{N}} \tilde{x}(\tau) \quad \text{and} \quad y(\tau) := 16^{\frac{1}{N}} \tilde{y}(\tau).$$

Now, $x(\tau)$ and $y(\tau)$ have rational Fourier coefficients, and we have that

$$x(\tau)^N - y(\tau)^N = -16. \tag{7.3}$$

For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and (weakly) modular form $f(\tau)$ of weight k define a slash operator

$$(f|\gamma)(\tau) := (c\tau + d)^{-k} f(\gamma\tau).$$

A straightforward calculation shows [14, §2]

$$\begin{aligned} (x|A)(\tau) &= \zeta_N x(\tau) \qquad & (x|B)(\tau) &= \zeta_N x(\tau), \\ (y|A)(\tau) &= \zeta_N x(\tau) \qquad & (y|B)(\tau) &= y(\tau), \end{aligned}$$

where ζ_N is a primitive Nth root of unity. Hence, $t(\tau) := \frac{x(\tau)}{y(\tau)}$ is invariant under $\Phi_0(N)$.

Modular curve $X(2)$ has three cusps: 0, 1, and ∞. There is one cusp of modular curve $X(\Phi_0(N))$ lying above cusps 0 and 1, and N cusps $\infty_1, \ldots, \infty_N$ lying above cusp ∞. As functions on $X(\Phi_0(N))$, $\tilde{\lambda}(\tau)$ and $1 - \tilde{\lambda}(\tau)$ have simples poles at ∞_i and zero of order N at cusps 0 and 1 respectively. Function $t(\tau)$ is holomorphic on $\mathbb{H}$, nonzero on cusps above infinity, has a pole of order one at cusp 1, and a zero of order one at cusp 0 ($t(\tau)$ is a hauptmoduln for $X(\Phi_0(N))$).

Denote by $S_3(\Phi_0(N))$ the space of cusp forms of weight 3 for $\Phi_0(N)$. It is well known that $\theta_1(\tau) := (\sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau})^2$ is a modular form of weight 1 for Δ. It has a zero at cusp 1 of order 1/2 (cusp 1 is irregular).

Let Γ be a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of genus g such that $-I \notin \Gamma$. For k odd, [13, Theorem 2.25] gives the following formula for the dimension of $S_k(\Gamma)$

$$\dim S_k(\Gamma) = (k-1)(g-1) + \frac{1}{2}(k-2)r_1 + \frac{1}{2}(k-1)r_2 + \sum_{i=1}^{j} \frac{e_i - 1}{2e_i},$$

where r_1 is the number of regular cusp, r_2 is the number of irregular cusps, and $e_i's$ are the orders of elliptic points. Since $\Phi_0(N)$ has no elliptic points (Δ is a free group), it follows that $\dim S_3(N) = \frac{N-1}{2}$.

Define $f_i(\tau) := \theta_1^3(\tau) t^i(\tau) \frac{1}{16(1-\tilde{\lambda}(\tau))}$ for $i = 1, 2, \dots N-1$. The divisor of $f_i(\tau)$ is

$$\mathrm{div}(f_i) = i(0) + (\frac{1}{2}N - i)(1) + \sum_{j=1}^{N}(\infty_j).$$

Hence $\{f_i(\tau)\}$, for $i = 1, \dots, \frac{N-1}{2}$, form a basis of $S_3(\Phi_0(N)$. If $i = \frac{N+1}{2}, \dots, N-1$, then $f_i(\tau)$ has a pole at cusp 1, and since the cusp 1 is irregular the constant Fourier coefficient is zero. It follows $f_i(\tau) \in S_3^{\mathrm{wk-ex}}(\Phi_0(N))$. Since $(t|B)(\tau) = \zeta_N t(\tau)$, it follows that $(f_i|B)(\tau) = \zeta_N^i f_i(\tau)$.

8 ℓ-adic representations

In this section we define two closely related compatible families of ℓ-adic Galois representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ attached to the space of cusp forms $S_3(\Phi_0(N))$. The first family $\rho_{N,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_N(\mathbb{Q}_\ell)$ is a ℓ-adic realisation of a motive associated to the space of cusp forms $S_3(\Phi_0(N))$. It is a special case of second author's construction from [10, Section 5]. For a more detailed description see [8, Section 5].

To describe the second family, consider an elliptic surface fibred over the modular curve $X(\Phi_0(N))$, defined by the following equation

$$\mathcal{E}^N : Y^2 = X(X+1)(X+t^N),$$

together with the map

$$h : \mathcal{E}^N \longrightarrow X(\Phi_0(N)),$$

mapping $(X, Y, t) \longmapsto t$. It was obtained from the Legendre's elliptic surface fibred over $X(2)$

$$\mathcal{E} : Y^2 = X(X-1)(X-\lambda),$$

by substituting $\lambda = 1 - t^N$. Note that λ corresponds to $\lambda(\tau) = 16q^{\frac{1}{2}} - 128q + 704q^{\frac{3}{2}} + \cdots$, the usual lambda modular function on $\Gamma(2)$, and we can check directly that

$$\lambda(\tau) = 1 - t(\tau)^N.$$

Map h is tamely ramified along cusp and elliptic points so following [8, Section 5] we define ℓ-adic Galois representation $\rho^*_{N,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_N(\mathbb{Q}_\ell)$ as follows.

Let $X(\Phi_0)^0$ be the part of $X(\Phi_0)$ with cusps and elliptic points removed. Denote by i inclusion of $X(\Phi_0)^0$ into $X(\Phi_0)$, and by $h' : \mathcal{E}_N \longrightarrow X(\Phi_0(N))^0$ the restriction map. For a prime ℓ we obtain a sheaf

$$\mathcal{F}_\ell = R^1 h'_* \mathbb{Q}_\ell$$

on $X(\Phi_0)^0$, and also a sheaf $i_*\mathcal{F}_\ell$ on $X(\Phi_0)$. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\mathbb{Q}_\ell$-space

$$W_\ell = H^1_{et}(X(\Phi_0) \otimes \overline{\mathbb{Q}}, i_*\mathcal{F}_\ell)$$

defines an ℓ-adic representation $\rho^*_{N,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_N(\mathbb{Q}_\ell)$.

Proposition 5.1 of [8] implies that the two representations $\rho^*_{N,\ell}$ and $\rho_{N,\ell}$ are isomorphic up to a twist by a quadratic character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

9 Jacobi sums and Grossencharacters of cyclotomic field

We review some results of Weil [15]. Let $m > 1$ be an integer, ζ_m a primitive m-th root of unity, and $\mathfrak{p}$ a prime ideal of $\mathbb{Q}(\zeta_m)$ relatively prime to m. For any integer t prime to m, $\zeta_m \to \zeta_m^t$ determines an automorphism σ_t of $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}$. Denote by q the norm of $\mathfrak{p}$. Hence $q \equiv 1 \pmod{m}$. For $x \in \mathbb{Q}(\zeta_m)$ prime to $\mathfrak{p}$ define $\chi_\mathfrak{p}(x)$ to be the unique m-th root of unity such that

$$\chi_\mathfrak{p}(x) \equiv x^{\frac{q-1}{m}} \pmod{\mathfrak{p}}.$$

It follows that $\chi_\mathfrak{p} : \mathbb{Z}[\zeta_m]/\mathfrak{p} \cong \mathbb{F}_q \longrightarrow \mu_m$ is a multiplicative character of order m.

Definition (Jacobi sum)**.** For a positive integer r and $a = (a_1, \ldots, a_r) \in \mathbb{Z}^r$ we define

$$J_a(\mathfrak{p}) := (-1)^r \sum_{\substack{x_1+\ldots+x_r \equiv -1 (\mathfrak{p}) \\ x_1,\ldots,x_r \bmod \mathfrak{p}}} \chi_\mathfrak{p}(x_1)^{a_1} \ldots \chi_p(x_r)^{a_r},$$

where sum ranges over complete set of representatives of congruence classes modulo $\mathfrak{p}$ in $\mathbb{Q}(\zeta_m)$. We extend the definition of $J_a(\mathfrak{a})$ to all ideals $\mathfrak{a}$ of $\mathbb{Q}(\zeta_m)$ prime to m by multiplicativity.

Let K be a number field and let $I_K = \prod'_\nu K^*_\nu$ be idele group of K. Recall that K^* embeds diagonally into I_K: $x \in K^* \mapsto (x_\nu)_\nu$, where x_ν is the image of x under the embedding of K into its completion at place ν, K_ν.

Definition (Grossencharacter)**.** A Grossencharacter ψ on K is a continuous homomorphism

$$\psi : I_K \longrightarrow \mathbb{C}^\times$$

which is trivial on $K^\times$. We say it is unramified at prime $\mathfrak{p}$ of K if $\psi(\mathcal{O}_\mathfrak{p}^\times) = 1$ where $\mathcal{O}_\mathfrak{p}$ is the ring of integers of $K_\mathfrak{p}$.

We can interpret Grossencharacter ψ as a homomorphism on the group of non-zero fractional ideal of K as follows. Let $\mathfrak{p}$ be a prime of K, let π be uniformizer of $K_{\mathfrak{p}}$, and let $\alpha_{\mathfrak{p}} \in I_K$ be the element which is π at the place $\mathfrak{p}$ and 1 at all other places. We define

$$\psi(\mathfrak{p}) = \begin{cases} \psi(\alpha_{\mathfrak{p}}) & \text{if } \psi \text{ is unramified at } \mathfrak{p}, \\ 0 & \text{otherwise.} \end{cases}$$

Definition. The Hecke L-series attached to a Grossencharacter ψ of K is given by the Euler product over all primes of K

$$L(\psi, s) = \prod_{\mathfrak{p}} \left(1 - \frac{\psi(\mathfrak{p})}{(N^K_{\mathbb{Q}}(\mathfrak{p}))^s}\right)^{-1}.$$

Theorem 9.1 (Weil, [15])**.** *For each $a \neq (0)$ the function $J_a(\mathfrak{a})$ is a Grossencharacter on $\mathbb{Q}(\zeta_m)$ of conductor dividing m^2. It is given by a formula*

$$J_a(\mathfrak{a}) = \mathfrak{a}^{\omega_m(a)},$$

where

$$\omega_m(a) = \sum_{\substack{(t,m)=1 \\ t \bmod m}} \left[\sum_{\rho=1}^{r} \left\langle \frac{t a_\rho}{m} \right\rangle\right] \sigma_t^{-1}.$$

(Here $\langle x \rangle$ is a fractional part of a rational number x.)

We will need the following technical lemma.

Lemma 9.2. *Let $N > 1$ be an odd integer, k and $d|N$ positive integers, $p \equiv 1 \pmod N$ a rational prime, $\mathfrak{p}$ a prime of $\mathbb{Z}[\zeta_{N/d}]$ above p, and $\tilde{\mathfrak{p}}$ a prime of $\mathbb{Z}[\zeta_{\frac{p^k-1}{d}}]$ above $\mathfrak{p}$. For simplicity write $\frac{p^k-1}{d} = 2NN'/d$. Let $J_{(2,N/d)}(\mathfrak{p})$ and $J_{(2N',NN'/d)}(\tilde{\mathfrak{p}})$ be Jacobi sums associated to fields $\mathbb{Q}(\zeta_{N/d})$ and $\mathbb{Q}(\zeta_{\frac{p^k-1}{d}})$ with defining ideals $2N/d$ and $(p^k-1)/d$ (i.e. characters $\chi_{\mathfrak{p}}$ and $\chi_{\tilde{\mathfrak{p}}}$ are of order $2N/d$ and $(p^k-1)/d = 2NN'/d$). We have*

$$\left(J_{(2,N/d)}(\mathfrak{p})\right)^{2k} = J_{(2N',NN'/d)}(\tilde{\mathfrak{p}})^2.$$

Proof. By Theorem 9.1 it is enough to prove that

$$\left(\prod_{\substack{(t,2N)=1 \\ t \bmod 2N}} \left[\left\langle \frac{2dt}{2N} \right\rangle + \left\langle \frac{Nt}{2N} \right\rangle\right] \sigma_t^{-1}(\mathfrak{p})\right)^k = \prod_{\substack{(t,2N'N)=1 \\ t \bmod 2N'N}} \left[\left\langle \frac{2dN't}{2N'N} \right\rangle + \left\langle \frac{N'Nt}{2N'N} \right\rangle\right] \sigma_t^{-1}(\tilde{\mathfrak{p}}).$$

Notice that the expressions in square rackets on both sides are the same, and only depend on $t \bmod 2N$. Moreover, $\tilde{\mathfrak{p}}$ has residual degree k (since the order of p in $\left(\mathbb{Z}/d(p^k-1)\mathbb{Z}\right)^\times$ is k), and p is unramified in $\mathbb{Q}(\zeta_{\frac{p^k-1}{d}})$. The lemma follows from an easy counting argument. ∎

10 Traces of Frobenius

To simplify notation, denote $\mathcal{F} = i_*\mathcal{F}_\ell$. The following theorem is well known.

Theorem 10.1. *$Tr(Frob_q|W_\ell)$ may be computed as follows*

(1)

$$Tr(Frob_q|W_\ell) = -\sum_{t\in X(\Phi_0(N))(\mathbb{F}_q)} Tr(Frob_q|\mathcal{F}_t).$$

(2) If the fiber $\mathcal{E}_t^N$ is smooth, then

$$Tr(Frob_q|\mathcal{F}) = Tr(Frob_q|H^1(\mathcal{E}_t^N, \mathbb{Q}_\ell)) = q + 1 - \#\mathcal{E}_t^N(\mathbb{F}_q).$$

(3) If the fiber $\mathcal{E}_t^N$ is singular, then

$$Tr(Frob_q|\mathcal{F}_t) = \begin{cases} 1 & \textit{if the fiber is split multiplicative,} \\ -1 & \textit{if the fiber is nonsplit multiplicative,} \\ 0 & \textit{if the fiber is additive.} \end{cases}$$

Theorem 10.2. *Let $N > 1$ be an odd integer, and ℓ a prime. Galois representations $\rho^*_{N,\ell}$ and $\oplus_{d|N} J^2_{(2,N/d)}$ have the same local factors over all primes $p \nmid 2N\ell$.*

Proof. Let k be a positive integer, p be an odd prime, and $q = p^k$ such that $q \equiv 1 \pmod N$. Let χ be any character of $\mathbb{F}_q^\times$ of order $2N$ (it exists since $q \equiv 1 \pmod{2N}$). We count the points on elliptic surface $\mathcal{E}^N$ (points at infinity are excluded).

$$\begin{aligned}\#\mathcal{E}^N(\mathbb{F}_q) &= \sum_{t\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q}\left(\chi^N(x(x+1)(x+t^N)) + 1\right) \\ &= q^2 + \sum_{x\in\mathbb{F}_q}\chi^N(x(x+1))\sum_{t\in\mathbb{F}_q}\chi^N(x+t^N).\end{aligned}$$

$$\begin{aligned}\sum_{t\in\mathbb{F}_q}\chi^N(x+t^N) = \left[\begin{smallmatrix} x_1 = t^N \\ x_2 = -x-t^N\end{smallmatrix}\right] &= \chi^N(x) + \sum_{x_1+x_2=-x}\ \sum_{\chi_N \text{ of order } |N} \chi_N(x_1)\chi^N(-x_2) \\ &= \chi^N(x) + \chi^N(-1)\sum_{i=1}^{N-1}\sum_{x_1+x_2=-x}\chi^{2i}(x_1)\chi^N(x_2).\end{aligned}$$

Define

$$\begin{aligned}
J_i(x) &:= \chi^N(-1) \sum_{x_1+x_2=-x} \chi^{2i}(x_1)\chi^N(x_2) \\
&= \begin{bmatrix} x_1=x_1'\cdot x \\ x_2=x_2'\cdot x \end{bmatrix} = \chi^N(-1) \sum_{x_1'+x_2'=-1} \chi^{2i}(x)\chi^{2i}(x_1')\chi^N(x)\chi^N(x_2') \\
&= \chi^N(-1)\chi^N(x)\chi^{2i}(x) \sum_{x_1'+x_2'=-1} \chi^{2i}(x_1'))\chi^N(x_2') \\
&= \chi^{2i}(x)\chi^N(x)J_i(1).
\end{aligned}$$

$$\begin{aligned}
\#\mathcal{E}^N(\mathbb{F}_q) &= q^2 + \sum_{x\in\mathbb{F}_q} \chi^N(x(x+1)) \left(\sum_{i=1}^{N-1} J_i(1)\chi^{2i}(x)\chi^N(x) + \chi^N(x) \right) \\
&= q^2 + \sum_{i=1}^{N-1} J_i(1) \left(\sum_{x\in\mathbb{F}_q} \chi^N(-x-1)\chi^N(-1)\chi^{2i}(x) + \sum_{x\in\mathbb{F}_q} \chi^N(x+1) \right) \\
&= q^2 + \sum_{i=1}^{N-1} J_i(1)^2.
\end{aligned}$$

Singular fibers of elliptic surface $\mathcal{E}^N$ are $\mathcal{E}_t^N$ where $t=0$ or $t^N=1$ (we call such t bad - the rest are called good). In the first case, $\mathcal{E}_0^N : y^2 = (x+1)x^2$ is the curve of split multiplicative type with $\#\mathcal{E}_0^N(\mathbb{F}_q) = q$ (counting the point at infinity). In the second case, $\mathcal{E}_t^N : y^2 = x(x+1)^2$ is the split multiplicative if $\chi^N(-1) = 1$ (or equivalently if $p \equiv 1 \pmod 4$), and nonsplit multiplicative if $\chi^N(-1) = -1$. It is easy to check that $\#\mathcal{E}_t^N(\mathbb{F}_q) = q+1-\chi_N(-1)$. Denote by M the number of Nth roots of unity in $\mathbb{F}_q$. Theorem 10.1 implies

$$\begin{aligned}
Tr(Frob_q|W_\ell) &= - \sum_{t\in X(\Phi_0(N))(\mathbb{F}_q)} Tr(Frob_q|\mathcal{F}_t) \\
&= \sum_{t \text{ good}} \#\mathcal{E}_t^N(\mathbb{F}_q) - (q+1)\cdot\#\{t \text{ good}\} - \sum_{t \text{ bad}} Tr(Frob_q|\mathcal{F}_t) \\
&= \#\mathcal{E}^N(\mathbb{F}_q) + \#\{t \text{ good}\} - \sum_{t \text{ bad}} (\#\mathcal{E}_t^N(\mathbb{F}_q) - 1) \\
&\qquad - (q+1)\#\{t \text{ good}\} - (\chi^N(-1)M + 1) \\
&= q^2 + \sum_{i=1}^{N-1} J_i(1)^2 - (q-1) - M(q - \chi^N(-1)) \\
&\qquad - q(q-1-M) - (\chi^N(-1)M + 1) \\
&= \sum_{i=1}^{N-1} J_i(1)^2
\end{aligned}$$

Assume that $p \equiv 1 \pmod{2N}$ (p splits completely in $\mathbb{Q}(\zeta_{2N})$). It is enough to show that $Tr(Frob_q|W_\ell) = \sum_{d|N}\sum_{\mathfrak{p}} J_{(2,N/d)}(\mathfrak{p})^{2k}$, where the second sum is over the primes of $\mathbb{Q}(\zeta_{2N/d})$ that are above p. Fix $d|N$. For any $\tilde{\mathfrak{p}}$ a prime of $\mathbb{Q}(\zeta_{\frac{p^k-1}{d}})$ above p the residual degree of $\tilde{\mathfrak{p}}$ in $\mathbb{Q}(\zeta_{\frac{p^k-1}{d}})$ is k (since the order of p in $\left(\mathbb{Z}/d(p^k-1)\mathbb{Z}\right)^\times$ is k), hence $\chi_{\tilde{\mathfrak{p}}}$ is a character of $\mathbb{F}_q^\times$ of order $\frac{p^k-1}{d}$. We can choose $\tilde{\mathfrak{p}}$ such that

$$J_{\left(\frac{p^k-1}{N},\frac{p^k-1}{2d}\right)}(\tilde{\mathfrak{p}})^2 = J_d(1)^2.$$

By Lemma 9.2 it follows

$$J_d(1)^2 = J_{(2,N/d)}(\mathfrak{p})^{2k},$$

where $\mathfrak{p}$ is the prime of $\mathbb{Q}(\zeta_{N/d})$ below $\tilde{\mathfrak{p}}$. Since $J_{dj}(1)^2$'s are conjugate to each other for $j = 1,\dots,N/d$ with $(j,N/d)=1$, it follows that

$$\sum_{(j,N/d)=1} J_{dj}(1)^2 = \sum_{\mathfrak{p}\text{ above }p} J_{(2,N/d)}(\mathfrak{p})^{2k}.$$

The claim follows after summing over $d|N$. Case $p \not\equiv 1 \pmod N$ is proved in the similar way. □

11 Atkin and Swinnerton-Dyer congruences

We apply results of §5 to obtain congruences of Atkin and Swinnerton-Dyer type between Fourier coefficients of (weakly) modular forms $f_i(\tau)$. Let $p > 3$ be a prime such that $p \nmid N$. Set $R = \mathbb{Z}_p$, and let $X = X(\Phi_0(N))$ and $X' = X(2)$ be curves over R. Let $g : X \longrightarrow X'$ be a finite morphism that extends the quotient map $\Phi_0(N)\backslash\mathbb{H} \longrightarrow \Gamma(2)\backslash\mathbb{H}$ (see proof of [10, Proposition 5.2 a)]). Denote by $W := DR(X,3)\otimes\overline{\mathbb{Q}}_p$ de Rham space corresponding to this data. The action of $B = \left(\begin{smallmatrix}1&0\\2&1\end{smallmatrix}\right)$ on the space of cusp forms $S_3(\Phi_0(N))$ extends to W(for $h^\vee \in S_3(\Phi_0(N))^\vee$ and $f \in S_3(\Phi_0(N))$ we have $(h^\vee|B)(f) = h^\vee(f|B^{-1})$). We write $W = \oplus_{i=1}^{N-1}W_i$, where W_i is the eigenspace of B corresponding to the eigenvalue ζ_N^i. Since $(f_i|B)(\tau) = \zeta_N^i f_i(\tau)$ for $i = 1,\dots,N-1$ and $f_i(\tau) \in S_3^{\mathrm{wk-ex}}(\Phi_0(N))$, Theorem 5.3 implies that $f_i(\tau) \in W_i$. Let ϕ be a linear endomorphism of W defined in §6.

Proposition 11.1. *For $i = 1,\dots,N-1$ we have that*

$$\phi(W_i) \subset W_{i\cdot p \bmod N}.$$

Proof. Since $B\phi = \phi B^p$ (see [9, Section 4.4]), for $f \in W_i$ we have

$$\phi(f)|B = \phi((f|B)^p) = \zeta_N^{ip}\phi(f),$$

and the claim follows. □

Define $\alpha_i \in \mathbb{Z}_p$ such that $\phi(f_i) = \alpha_i f_{i\cdot p \bmod N}$.

Proposition 11.2.

$$\mathrm{ord}_p(\alpha_i) = \begin{cases} 2 & \text{if } i = 1, \ldots \frac{N-1}{2}, \\ 0 & \text{if } i = \frac{N+1}{2}, \ldots, N-1. \end{cases}$$

Proof. Proposition 3.4 of [10] implies

$$\phi(S_3(\Phi_0(N))) \subset p^2 DR(X, 3).$$

Since f_i's are normalized, it follows that $\mathrm{ord}_p(\alpha_i) \geq 2$, for $i = 1, \ldots, \frac{N-1}{2}$. On the other hand, determinant of ϕ is $\pm p^{2 \dim S_3(\Phi_0(N))} = \pm p^{N-1}$, hence $\mathrm{ord}_p(\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_{N-1}) = N - 1$ and the claim follows. $\square$

Let $f_i(\tau) = q^{1/2} + \sum_{j=1}^{\infty} a_i(j) q^{\frac{j}{2}}$, for $i = 1, \ldots, N-1$. From the description of the action of ϕ (6.1) on the de Rham space $DR(X, 3)$ (and $DR(X, 3)^{(p)}$ when f_i is a cusp form, see §2), it follows

Corollary 11.3. *For $i = 1, \ldots, N-1$ and positive integer j, we have that*

$$\frac{p^2}{\alpha_i} a_i(j) \equiv a_{i\cdot p \bmod N}(pj) \pmod{p^{2(\mathrm{ord}_p(j)+1)}}.$$

Suppose Γ is a noncongruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of finite index such that modular curve $X(\Gamma)$ has a model over $\mathbb{Q}$ (see §2). Based on Atkin and Swinnerton-Dyer discovery, Li, Long, and Yang conjectured (Conjecture 1.1 of [8]) that for every integer $k \geq 2$, there exist a positive integer M such that for every prime $p \nmid M$ there is a basis of $S_k(\Gamma)$ consisting of M-integral forms $h_i(\tau)$, $1 \leq i \leq d := \dim S_k(\Gamma)$, algebraic integers $A_p(i)$, and characters χ_i such that for each i Fourier coefficients of $h_i(\tau) = \sum_j a_i(j) q^{\frac{j}{\mu}}$ (μ is the width of the cusp at infinity) satisfy the congruence relation

$$a_i(np) - A_p(i) a_i(n) + \chi_i(p) p^{k-1} a_i(n/p) \equiv 0 \pmod{p^{(k-1)(1+\mathrm{ord}_p(n))}},$$

for all $n \geq 1$. Second author in [10] associated to $S_k(\Gamma)$ a compatible family of ℓ-adic representations ρ_ℓ, and established congruences for $d = 1$. Moreover, it follows from his work that if Atkin and Swinnerton-Dyer (ASD) congruences hold for $S_k(\Gamma)$ for prime p, then

$$H_p(T) = \prod_{1 \leq i \leq d} (T^2 - A_p(i) T + \chi_i(p) p^{k-1}),$$

where $H_p(T)$ is the characteristic polynomial of $\rho_\ell(Frob_p)$.

Theorem 11.4. *Let $p \equiv 2, 3 \pmod 5$ be a prime. There is no basis of $S_3(\Phi_0(5))$ satisfying Atkin and Swinnerton-Dyer congruence relations for p.*

Proof. Assume that $\{g_1(\tau), g_2(\tau)\}$ is a normalized basis satisfiying ASD congruences. Theorem 10.2 implies that ρ_ℓ, the ℓ-adic representation attached to $S_3(\Phi_0(5))$, is isomorphic to the quadratic twist of Grossencharacter of $\mathbb{Q}(\zeta_5)$. In particular, since p is inert in $\mathbb{Q}(\zeta_5)$, we have that $H_p(T) = T^4 \pm p^4$. If ASD congruences hold for p, then corresponding $A_p(1)$ and $A_p(2)$ are divisible by p, so p-th Fourier coefficient of $g_1(\tau)$ and $g_2(\tau)$ is divisible by p, hence p-th Fourier coefficient of $f_1(\tau)$ and $f_2(\tau)$ is divisible by p. Propositions 11.2 implies that either $\phi(f_1(\tau)) = \alpha_1 f_2(\tau)$ or $\phi(f_2(\tau)) = \alpha_2 f_1(\tau)$, and $\mathrm{ord}_p(\alpha_1) = \mathrm{ord}_p(\alpha_2) = 0$. It follows from Corollary 11.3 that p-th Fourier coefficient of $f_1(\tau)$ or $f_2(\tau)$ is not divisible by p which is in contradiction with our assumption. □

Remark. J. Kibelbek [7] provided an example of the space of weight two modular forms that does not admit a basis satisfying Atkin and Swinnerton-Dyer congruence relations.

References

[1] A. O. L. Atkin, W.-C. W. Li, L. Long *On Atkin-Swinnerton-Dyer congruence relations(2)* Math. Ann. **340** (2008), no. 2, 335–358.

[2] A. O. L. Atkin, H. P. F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups* Combinatorics, (Proc. Sympos. Pure Math., Vol. XIX, Univ. Californis, Los Angeles, 1968), Amer. Math. Soc., 1–25.

[3] P. Cartier, *Groupes formels, fonctions automorphes et fonctions zeta des courbes elliptiques* Actes du Congrs International des Mathmaticiens (Nice, 1970), Tome **2**, 291-299.

[4] P. Deligne, *Equations differentielles a points singuliers reguliers*, Lecture Notes in Mathematics, Vol. 163. Springer-Verlag, Berlin-New York, 1970.

[5] B. Ditters, *Sur les congruences d'Atkin et de Swinnerton-Dyer*, C. R. Acad. Sci. Paris Sr. A-B **282** (1976), no. 19, Ai, A1131A1134.

[6] N.M. Katz *p-adic properties of modular schemes and modular forms* Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Mathematics, Springer, Berlin, 1973, Vol. **350**, 69-190.

[7] J. Kibelbek *On Atkin-Swinnerton-Dyer congruence relations for noncongruence subgroups* Proc. Amer. Math. Soc., to appear.

[8] W.-C. W. Li, L. Long, Z. Yang *On Atkin-Swinnerton-Dyer congruence relations* J. Number Theory **113** (2005), no. 1, 117–148.

[9] L. Long *On Atkin-Swinnerton-Dyer congruence relations (3)* J. Number Theory **128** (2008), no. 8, 2413–2429.

[10] A. J. Scholl, *Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences* Invent. Math. **79** (1985), 49–77.

[11] A. J. Scholl, *Motives for modular forms* Invent. Math. **100** (1990), no. 2, 419-430.

[12] D. Rohrlich, *Points at infinity on the Fermat curves* Invent. Math. **39** (1977), 95–127.

[13] G.Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kano Memorial Lectures, no. 1. Publications of the Mathematical Society of Japan, no. 11.

[14] T. Yang, *Cusp form of weight 1 associated to Fermat curves* Duke Math J. **83** (1996), 141–156.

[15] A. Weil, *Jacobi sums as "Grössencharaktere"* Trans. Amer. Math. Soc. **73**, (1952). 487-495.

Department of Mathematics
University of Zagreb
Bijenicka cesta 30
Zagreb, Croatia
mkazal@math.hr

Department of Pure Mathematics and Mathematical Statistics
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB
a.j.scholl@dpmms.cam.ac.uk